UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,667	02/05/2004	Mukesh Kumar Singh	TI-35979	5588

23494 7590 08/13/2009

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
DEBNATH, SUMAN	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
08/13/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@ti.com

Office Action Summary	Application No.	Applicant(s)	
	10/772,667	SINGH, MUKESH KUMAR	
	Examiner	Art Unit	
	SUMAN DEBNATH	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-13,15 and 16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-13,15 and 16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3-13 and 15-16 are pending in this application.

2. Claims 1, 4, 9 and 13 are currently amended.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 24, 2009 has been entered.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1, 3-8 and 13 are rejected under 35 U.S.C. 102(e) as being anticipated by Kuhlman (Pub. No.: US 2003/0086564 A1).

2. As to claim 1, Kuhlman discloses a method of encryption, of a digital signal processor, comprising:

Preprocessing, in said digital signal processor, an input message wherein said preprocessing includes a permutation of said input message ("Each s-box subround contains a permutation polynomial function 110 with modulo reduction and a hilo split 120", e.g. see, [0021], see also FIG. 2, 3 and [0023], [0030]);

partitioning said input message into matrix elements, where said matrix is a square matrix, and diagonally filling said matrix ("The 128 bit wide cipher input 210 is split into four thirty-two bit paths for processing. Each of the four paths is first pre-whitened 220 before the rounds in the block cipher of FIG. 2" , e.g., see, [0023], see also "a matrix convolution 250 is performed on the outputs Ba, Bb, Bc and Bd of all four of the s-boxes 100 to generate Ya, Yb, Yc and Yd.", e.g. see, [0025], see also, FIG. 2, 3 and [0023], [0030]);

computing a determinant of said matrix ("Continuing with the description of FIG. 2, a matrix convolution 250 is performed on the outputs Ba, Bb, Bc and Bd of all four of the s-boxes 100 to generate Ya, Yb, Yc and Yd. The matrix convolution 250 will further be described below in accordance with FIG. 9. Finally, whitening XOR operations 261, 262, 263 and 264 against the keys are performed on the results Ya, Yb, Yc and Yd of the matrix convolution 250.", e.g. see, [0025], FIG. 2, 3);

public key encrypting said determinant ("whitening XOR operations 261, 262, 263 and 264 against the keys are performed on the results Ya, Yb, Yc and Yd of the matrix convolution 250", e.g. see, [0025], see also, FIG. 2, 3, [0021], [0023], [0030],; and

multiplying said matrix by said encrypted determinant ("At the end of each of the four rounds 221, 222, 223 and 224, the keys k0, k1, k2 or k3 are used in the XOR operations in different orders as illustrated to increase cipher strength. In the second round 222, extra pre-XOR operations 271, 272 and 273 are performed with an arbitrary integer on keys k2, k3 and k1 to further increase strength", e.g. see, [0026], see also, FIG. 2, 3, [0021], [0023], [0025], [0030]).

3. As to claim 3, Kuhlman discloses said permutation is generated by a hash of said input message (FIG. 2, 3, [0021], [0023], [0025], [0026], [0030]).

4. As to claim 4, Kuhlman discloses said permutation is generated by a random sequence (FIG. 2, 3, [0021], [0023], [0025], [0026], [0030]).

5. As to claim 5, Kuhlman discloses said preprocessing comprises exclusive ORing said message after permutation with generators of said permutation (FIG. 2, 3, [0021], [0023], [0025], [0026], [0030]).

6. As to claim 6, Kuhlman discloses said encrypting is public-key encryption (FIG. 2, 3, [0021], [0023], [0025], [0026], [0030]).

7. As to claim 7, Kuhlman discloses said public-key encryption is RSA (FIG. 2, 3, [0021], [0023], [0025], [0026], [0030]).

8. As to claim 8, Kuhlman discloses said partitioning first fills the principal diagonal of said matrix (FIG. 2, 3, [0021], [0023], [0025], [0026], [0030]).

9. As to claim 13, it is rejected using the similar rationale as for the rejection of claim 1.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 9-12 and 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guski et al. (Patent No.: 5,592,553) (hereinafter, "Guski") and further in view of Kuhlman.

12. As to claim 9, Guski discloses a method of encryption for a digital signal processor, comprising

preprocessing said input message wherein said preprocessing includes a permutation of said input message and defining a permutation source ("the right input half R2B is first permuted (step 1004) according to Permutation Table (7-n) (block 1110), where n is the number of the round or loop count, to produce a permuted right

input half R2B (1112). For example, for the first time through (n=1), Permutation Table 6 is used.", e.g. see, col. 15, lines 34-48 to col. 16, lines 1-12);

generating a permuted message for an input message employing said permutation source ("the right input half R2B is first permuted (step 1004) according to Permutation Table (7-n) (block 1110), where n is the number of the round or loop count, to produce a permuted right input half R2B (1112). For example, for the first time through (n=1), Permutation Table 6 is used.", e.g. see, col. 15, lines 34-48 to col. 16, lines 1-12);

padding said permuted message with said permutation source to obtain a preprocessed message ("L2B (2 bytes) is concatenated (step 1006) with 6 bytes of padding bits 1114 consisting of hexadecimal X'555555555555' to form an 8-byte (64-bit) quantity L8B (1116), such that the 2 bytes of L2B occupy the leftmost 2 byte positions of L8B. L8B is encrypted (step 1008) using DES (block 1118)", e.g. see, col. 15, lines 34-48 to col. 16, lines 1-12); and

encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message ("L2B (2 bytes) is concatenated (step 1006) with 6 bytes of padding bits 1114 consisting of hexadecimal X'555555555555' to form an 8-byte (64-bit) quantity L8B (1116), such that the 2 bytes of L2B occupy the leftmost 2 byte positions of L8B. L8B is encrypted (step 1008) using DES (block 1118)", e.g. see, col. 15, lines 34-48 to col. 16, lines 1-12).

Guski doesn't explicitly disclose partitioning said input message into matrix elements, wherein said matrix is a square matrix, and diagonally filling said matrix;

However, Kuhlman discloses partitioning said input message into matrix elements ("The 128 bit wide cipher input 210 is split into four thirty-two bit paths for processing. Each of the four paths is first pre-whitened 220 before the rounds in the block cipher of FIG. 2" , e.g., see, [0023], see also "a matrix convolution 250 is performed on the outputs Ba, Bb, Bc and Bd of all four of the s-boxes 100 to generate Ya, Yb, Yc and Yd.", e.g. see, [0025], see also, FIG. 2, 3 and [0023], [0030]), wherein said matrix is a square matrix, and diagonally filling said matrix ("The 128 bit wide cipher input 210 is split into four thirty-two bit paths for processing. Each of the four paths is first pre-whitened 220 before the rounds in the block cipher of FIG. 2" , e.g., see, [0023], see also "a matrix convolution 250 is performed on the outputs Ba, Bb, Bc and Bd of all four of the s-boxes 100 to generate Ya, Yb, Yc and Yd.", e.g. see, [0025], see also, FIG. 2, 3 and [0023], [0030]);

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Guski as taught by Kuhlman in order to maintain higher level of security to an encryption algorithm while decryption processing time is faster.

13. As to claim 10, Guski discloses said permutation source is generated by a hash of said input message (e.g. see, col. 15, lines 34-48 to col. 16, lines 1-12).

14. As to claim 11, Guski discloses said permutation source is generated by a random sequence (e.g. see, col. 15, lines 34-48 to col. 16, lines 1-12).

15. As to claim 12, Guski discloses said block-based encryption is a public key encryption (e.g. see, col. 15, lines 34-48 to col. 16, lines 1-12).

16. As to claim 15, Guski discloses said padding includes pre-pending said permuted message with said permutation source to obtain said preprocessed message (e.g. see, col. 15, lines 34-48 to col. 16, lines 1-12).

17. As to claim 16, Guski discloses said padding includes appending said permuted message with said permutation source to obtain said preprocessed message (e.g. see, col. 15, lines 34-48 to col. 16, lines 1-12).

18. **Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the Applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Response to Arguments

19. Applicant's arguments filed July 24th, 2009 have been fully considered but they are not persuasive.

20. Applicant stated: "Guski "pre-processing, in said digital signal processor, an input message wherein said preprocessing includes a permutation of said input message and defining a permutation source partitioning said input message into matrix elements, wherein said matrix is a square matrix, and diagonally filling said matrix," as recited in claim 9."

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., wherein said matrix is a square matrix, and diagonally filling said matrix) were not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, Kuhlman discloses wherein said matrix is a square matrix, and diagonally filling said matrix ("The 128 bit wide cipher input 210 is split into four thirty-two bit paths for processing. Each of the four paths is first pre-whitened 220 before the rounds in the block cipher of FIG. 2" , e.g., see, [0023], see also "a matrix convolution 250 is performed on the outputs Ba, Bb, Bc and Bd of all four of the s-boxes 100 to generate Ya, Yb, Yc and Yd.", e.g. see, [0025], see also, FIG. 2, 3 and [0023], [0030], it should be noted that Kuhlman teaches

the above limitation because determinant of a matrix can be computed only from a square matrix and only when matrix is diagonally filled.).

21. Applicant argues that: "Kuhlman is devoice from disclosing "partitioning said input message into matrix elements, wherein said matrix is a square matrix, and diagonally filling said matrix," as recited in claim 1. Claim 13 recites similar features as those recited in claim 1. "

Examiner maintain that Kuhlman discloses wherein said matrix is a square matrix, and diagonally filling said matrix ("The 128 bit wide cipher input 210 is split into four thirty-two bit paths for processing. Each of the four paths is first pre-whitened 220 before the rounds in the block cipher of FIG. 2" , e.g., see, [0023], see also "a matrix convolution 250 is performed on the outputs Ba, Bb, Bc and Bd of all four of the s-boxes 100 to generate Ya, Yb, Yc and Yd.", e.g. see, [0025], see also, FIG. 2, 3 and [0023], [0030], it should be noted that Kuhlman teaches the above limitation because determinant of a matrix can be computed only from a square matrix and only when matrix is diagonally filled.)

Conclusion

22. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435